038 0116-1

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１１月　５日

出願番号
Application Number: 特願２００２－３２１３５５

[ST.10/C]: [ＪＰ２００２－３２１３５５]

出願人
Applicant(s): 株式会社東芝

２００３年　１月３１日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３００２８１４

【書類名】　特許願
【整理番号】　A000205169
【提出日】　平成14年11月 5日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 13/00
【発明の名称】　通信装置及び通信方法
【請求項の数】　20
【発明者】
【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
【氏名】　小久保　隆
【発明者】
【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
【氏名】　奥山　武彦
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置及び通信方法

【特許請求の範囲】

【請求項１】

非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施すパディング処理部と、

前記パディング処理部によりパディング処理されたパディング非同期パケット及び同期パケットを暗号化する暗号部と、

前記暗号部により暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信する送信部と、

を具備することを特徴とする通信装置。

【請求項２】

前記非同期パケットの実データの長さに関するデータ長情報を、前記暗号化パディング非同期パケットに付加するデータ長情報付加回路を更に有する請求項１記載の通信装置。

【請求項３】

前記暗号部で行う暗号化処理に用いる鍵情報を鍵書換情報に基づいて書き換え、前記鍵書換情報を前記暗号化パディング非同期パケットに付加する鍵管理部を更に有する請求項１記載の通信装置。

【請求項４】

少なくとも前記非同期パケットのコピー回数を制限するコピー制御情報を、前記暗号化パディング非同期パケットに付加するコピー制御情報付加回路を更に有する請求項１記載の通信装置。

【請求項５】

前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号部で行う暗号化処理に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして、前記暗号化パディング非同期パケットの列の中に挿入する付加回路を更に有する請求項１記載の通信装置。

【請求項６】

前記送信部から送信された前記暗号化パディング非同期パケットを受信する受信部と、

前記受信部が受信した前記暗号化パディング非同期パケットを復号して、前記パディング非同期パケットを出力する復号部と、

前記復号部が出力した前記パディング非同期パケットから、前記パディング処理部で付加したデータを除いて実データを抽出する抽出部と、

を具備することを特徴とする請求項１記載の通信装置。

【請求項７】

前記抽出部は、前記非同期パケットの実データの長さに関するデータ長情報を検出し、これに基づいて、前記復号部が出力した前記パディング非同期パケットから、前記付加したデータを除いて実データを抽出することを特徴とする請求項６記載の通信装置。

【請求項８】

前記復号部は、前記暗号部で行う暗号化処理に用いる鍵情報を書き換える鍵書換情報を検出し、これにより書き換えた最新の鍵情報に基づいて、前記受信部が受信した前記暗号化パディング非同期パケットを復号することを特徴とする請求項６記載の通信装置。

【請求項９】

前記受信部が受信した前記非同期パケットのコピー回数を制限するコピー制御情報を検出し、この制限の範囲内で、少なくとも前記非同期パケットをコピーするコピー機能を更に有する請求項６記載の通信装置。

【請求項１０】

前記受信部は、前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号部で行う暗号化処理に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして受信することを特徴とする請求項６記載の通信装置。

【請求項１１】

非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施し、

前記パディング処理されたパディング非同期パケット及び同期パケットを暗号化し、

前記暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信することを特徴とする通信方法。

【請求項１２】

前記非同期パケットの実データの長さに関するデータ長情報を、前記暗号化パディング非同期パケットに付加することを特徴とする請求項１１記載の通信方法。

【請求項１３】

前記暗号化に用いる鍵情報を鍵書換情報に基づいて書き換え、前記鍵書換情報を前記暗号化パディング非同期パケットに付加することを特徴とする請求項１１記載の通信方法。

【請求項１４】

少なくとも前記非同期パケットのコピー回数を制限するコピー制御情報を、前記暗号化パディング非同期パケットに付加することを特徴とする請求項１１記載の通信方法。

【請求項１５】

前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号化に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして、前記暗号化パディング非同期パケットの列の中に挿入することを特徴とする請求項１１記載の通信方法。

【請求項１６】

前記送信された前記暗号化パディング非同期パケットを受信し、これを復号して、前記パディング非同期パケットを出力し、

前記パディング非同期パケットから前記付加したデータを除いて実データを抽出することを特徴とする請求項１１記載の通信方法。

【請求項１７】

前記非同期パケットの実データの長さに関するデータ長情報を検出し、これに基づいて、前記復号されたパディング非同期パケットから、前記付加したデータを除いて実データを抽出することを特徴とする請求項１６記載の通信方法。

【請求項１８】

前記暗号化に用いる鍵情報を書き換える鍵書換情報を検出し、これにより書き換えた最新の鍵情報に基づいて、前記受信した前記暗号化パディング非同期パケットを復号することを特徴とする請求項１６記載の通信方法。

【請求項１９】

前記非同期パケットのコピー回数を制限するコピー制御情報を検出し、この制限の範囲内で、少なくとも前記非同期パケットをコピーすることを特徴とする請求項１６記載の通信方法。

【請求項２０】

前記非同期パケットの実データの長さに関するデータ長情報と、前記暗号化に用いる鍵情報の書き換えのための鍵書換情報と、前記非同期パケットのコピー回数を制限するコピー制御情報との内の少なくとも一つの制御情報を、専用の制御情報パケットとして受信することを特徴とする請求項１６記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、パケット通信を行う通信装置であって、特に、非同期パケットを暗号化してパケット通信を行う通信装置及び通信方法に関する。

【０００２】

【従来の技術】

最近、多様なデジタル機器の開発・普及が広範に進み、これに応じて、デジタル機器同士の通信機能への要望も高まりつつある。すなわち、例えば、ＩＥＥＥ（Institute of Electrical Electronics Engineers）１３９４等の通信機能をもったＤＴＶ（Digital Television）やＤＶＤ（Digital Versatile Disk）プレイヤ等が一般化してきている。

【０００３】

これに関連した従来技術として、扱うデジタル情報の複写機能をもったデジタル機器を示す例がある（例えば、特許文献１参照）。ここでは、所定のデータフォーマットからコピー世代管理情報を検出する手段と、所定のデータフォーマットをネットワークバスのパケットフォーマット変換手段を含み、検出したコピー管理情報を変換手段による変換後のパケットフォーマットの所定位置に挿入してネットワークバスに送出する送信側インタフェースをもったデジタル機器が示されている。ここでは、同期式パケットとは明言されていないが、一例として、ＩＥＥＥ１３９４の同期パケットに適用するものと考えられる。

しかしながら、ここでは、非同期パケットを暗号化する手法が述べられてはいない。従って、ＤＴＣＰ（Digital Transmission Content Protection）暗号化方式等で同期パケットを暗号化している場合、非同期パケットの情報（例えば、画像情報等）については、同期パケットと一緒に暗号化を行うことができないため、セキュリティを保つことができない。

【０００４】

【特許文献１】

特開平０８－１８４８８１号公報。

【０００５】

【発明が解決しようとする課題】

すなわち、従来の通信装置においては、同期パケットに施されるブロック暗号等の暗号処理を、データ長が異なるために非同期パケットにはそのまま用いることができないので、同期パケットと非同期パケットが混在するデジタル機器においては，同期パケットのみについてブロック暗号が施され、非同期パケットは暗号化されることなく通信されてしまう。これにより、非同期パケットについては、第三者による不正複写に対してセキュリティが保てないという問題がある。

本発明は、非同期パケットも同期パケットと同様に暗号化して通信を行う通信装置及び通信方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

本発明は、非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施すパディング処理部と、前記パディング処理部によりパディング処理されたパディング非同期パケット及び同期パケットを暗号化する暗号部と、前記暗号部により暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信する送信部とを具備することを特徴とする通信装置である。

【０００７】

ＤＴＣＰ暗号化方式のように一定のブロック長によるブロック暗号により、同期パケットを暗号化して、ＩＥＥＥ１３９４等で他のデジタル機器と通信を行っているデジタル機器において、非同期パケットは、一定のブロック長をもっていないので、一律には暗号化処理を行うことができない。本発明に係る通信装置では、パディング処理により非同期パケットの実データに無効データ等を付加することで、暗号化方式が必要とするブロック長をもたせることにより、非同期パケットも同期パケットと同様に暗号化することができる。これにより、非同期パケットによりデータも同期パケットと同様に暗号化して、他のデジタル機器との間の通信を行うことが可能となる。

【０００８】

【発明の実施の形態】

以下、図面を参照してこの発明の実施形態である通信装置を詳細に説明する。図１は、本発明に係る通信装置であるテレビジョンの構成の一例を示すブロック図、図２は、本発明に係る通信装置により非同期パケットに施されるパディング処理を説明する図、図３は、パディング処理された非同期パケットに制御情報を付加することを説明する図、図４は、パディング処理された非同期パケットに制御情報の専用非同期パケットを付加することを説明する図、図５は、非同期パケットをパディング処理して送信処理する動作を説明するフローチャート、図６は、パディング処理された非同期パケットを受信処理する動作を説明するフローチャート、図７は、本発明に係る通信装置により構成されたネットワークシステムの一例を示すシステム図である。

【０００９】

＜通信装置とネットワークシステムの構成＞

本発明に係る通信装置は、例えば、デジタルテレビ等のデジタル機器であり、例えば、ＩＥＥＥ１３９４等の通信機能をもった通信装置である。ここでは、転送される情報はパケット形式で扱われ、同期パケットと非同期パケットとに分けることができる。

【００１０】

図１において、通信装置Ｎ２は、デジタルテレビの本来の機能、すなわち、同調回路や復号回路、映像処理回路や、オーディオ増幅部等の働きを総称する信号処理部１１と、映像を表示するための表示部１０との他に、通信機能として、ブロック暗号化処理をおこなうＤＴＣＰ部１２と、これに含まれる非同期パケット・鍵管理部１３とを有している。更に、通信装置Ｎ２は、先の信号処理部１１とＤＴＣＰ部１２とにデータバスでそれぞれ接続されており、送信すべき非同期パケットを扱う非同期処理部／パディング処理部１４と、受信した非同期パケットを扱う非同期処理部／抽出部１５と、同期パケットを扱う同期処理部１６と、パケットにデータ長情報及びコピー情報等を付加するためのデータ長情報・コピー情報付加回路１７と、送信部・受信部１８とを有している。

又、更に、本発明に係る通信装置は、ネットワークＮで複数のデジタル機器にそれぞれ接続されるネットワークを構成するものであり、図７のシステム図は、このネットワークを示している。すなわち、本発明に係る通信装置は、図７において、ネットワークＮにそれぞれ接続される、ＤＶＤプレイヤＮ１と、ＤＴＶＮ２と、ＰＣ（Personal Computer）Ｎ３と、ＤＴＶＮ４と、ＤＶＨＳＮ５と、プリンタＮ６とにより構成されるネットワークシステムに適用することができる。

【００１１】

ここでは、一例として、ＩＥＥＥ１３９４を通信規約とするパケット通信を行っているが、この通信規約に限ることなく、他のネットワーク通信の通信規約を用いるものであっても可能である。

＜本発明に係る通信動作及びパディング処理動作＞

次に、上述した本発明に係る通信装置の通信動作及び本発明に特有のパディング処理動作を、パケットを示すタイミングチャート及びフローチャートを用いて

詳細に説明する。

初めに、同期パケットと非同期パケットとの相違について述べる。同期パケットは、主に、動画映像データや音声データであることが多く、パケットの伝送に時間上の制約がある。又、送信側と受信側とで時刻あわせができる。又、リアルタイムの伝送用パケットであり、パケットの実データ部分の長さが固定値の整数倍である等の特徴をもっている。又、非同期パケットは、主に、制御データや静止画データであり、時刻の制約はなく、非リアルタイム伝送であり、可変調であるとの特徴をもっている。

ここで、図１に示すＤＴＶ（Digital Television）Ｎ２の表示部１０及び信号処理部１１は、本来のデジタルテレビの構成であり、外部からの放送信号を受信しこれを復調して映像信号を出力し、これに応じた映像を表示部１０に表示する。

更に、付随する通信機能を用いて、例えば、この映像信号を同期パケットとして、図７に示すＤＶＨＳＮ５へと、例えば、ＩＥＥＥ１３９４の通信規約に応じて送信する。又は、例えば、映像信号の一部である静止画信号を非同期パケットとして、図７に示すプリンタＮ６へと送信する。以下、フローチャートを用いて、送信動作及び受信動作を詳細に説明する。

（送信動作）

初めに、図５のフローチャートにおいて、パケット通信を行う対象が同期パケットか、非同期パケットかが判断される（Ｓ１１）。同期パケットであれば、図２に示すように、信号処理部１１から供給された予め決められたブロック長の整数倍の長さの同期パケットP_Sが、ＤＴＣＰ部１２に供給され、ブロック暗号化される（Ｓ１７）。そして、同期処理部１６により処理された後に、送信部１８を介して、ネットワークＮ上の他の通信装置、例えば、ＤＶＨＳＮ５へと供給される（Ｓ１８）。

【００１２】

一方、パケット通信を行う対象が非同期パケットであると判断されると（Ｓ１１）、図２に示すように、非同期パケットの実データＪがブロック長の整数倍の長さかどうかが判断される（Ｓ１２）。ここで、非同期パケットがブロック長の整

数倍であれば、特にパディング処理を施すことなくそのまま、ＤＴＣＰ部１２に供給されてブロック暗号化される（Ｓ１４）。ここで、非同期パケットがブロック長の整数倍でなければ、パディング処理部１４により、パディング処理が施され、図２に示すように、非同期パケットP_Nは、実データＪに付加データＤが付加されることでパディング処理される。こうしてブロック長の整数倍（又は２倍）の長さに調整され、以降のＤＴＣＰ部１２のブロック暗号化に備える（Ｓ１３）。そして、パディング処理された非同期パケットP_{N2}は、ＤＴＣＰ部１２に供給され、ブロック暗号化される（Ｓ１４）。

【００１３】

その後、同期パケットと同様に暗号化された非同期パケットP_{N2}は、図３に示すように、データ長情報付加回路１７により、実データＪのデータ長情報Ｌを、例えば、ヘッダＨの後に付加される（Ｓ１５）。その後、送信部１８に送られ、ネットワークＮを介して、例えば、プリンタＮ６に送信される（Ｓ１６）。

こうすることにより、本発明に係る通信装置によれば、非同期パケットの情報も同期パケットと同様に、ブロック暗号等の暗号化を施してセキュリティを確保しつつ通信処理を行うことが可能となる。

又、更に、図３に示すように、非同期パケットに、例えば、ＤＴＣＰ部１２で暗号化に用いられる暗号鍵をそのまま使用するのではなく、例えば、時間に応じてこの暗号鍵を書き換える鍵書換情報Ｋに基づき、鍵管理部１３により暗号鍵を書き換えて暗号化を行う。そして、この鍵書換情報Ｋを、図３に示すように、ヘッダＨの後に付加することも好適である。こうすることにより、非同期パケットについても同期パケットと同様に、時変鍵を使用して暗号化を行うことができるため、同期パケットと同様の手法で暗号化・復号処理が可能となる。

なお、鍵書換情報Ｋは、一例として、時変鍵がいつ変わったかを示す時刻情報であってもよいし、時変鍵が変わったことを示すフラグであってもよく、又、鍵を書き換えるための暗号情報であってもよく、様々な形態が可能である。この鍵書換情報Ｋは、同期パケットと非同期パケットとで共通していること好適である。

【００１４】

又、更に、パケット情報のコピー回数を、例えば、１回又は０回に制限する等のコピー制御情報Ｃを、非同期パケットP_{N2}のヘッダＨの後に付加することも好適である。このコピー制御情報は、例えば、２ビットの情報により、許容されるコピー回数等を特定している。これにより、非同期パケットについても同期パケットと同様に、コンテンツの複写回数を制限することで、コンテンツの著作権を一定の範囲で保護することが同期パケットと同様の手法で可能となる。

又、更に、図４に示すように、これらのデータ長情報Ｌ、鍵書換情報Ｋ、コピー制御情報Ｃの制御情報は、図３に示すように必ずしもヘッダＨの後に付加する必要はなく、例えば、データ長情報・コピー制御情報付加回路１７の働きにより、制御情報のための専用パケットP_{N3}を用意して、これを、非同期パケットP_{N2}の間に挿入することも好適である。これにより、同様に、非同期パケットも同期パケットと同様の手法により、時変鍵を用いた暗号化・復号処理及びコピー処理の制御を行うことが可能となる。

（受信動作）

このような動作により送信された同期パケット及び非同期パケットは、ネットワークＮを介して、他の通信装置により受信され、以下のように受信動作が行われる。

すなわち、図６のフローチャートにおいて、受信部１８により通信パケットを受信すると（Ｓ２１）、同期パケットか非同期パケットかが判断される（Ｓ２２）。同期パケットP_Sであれば、同期処理部１６により、ヘッダＨ等から制御情報を抽出する処理等が施された後に、ＤＴＣＰ部１２へと供給され、ブロック暗号により暗号鍵に基づいて復号される。暗号処理が時変鍵を用いられたものであれば、ヘッダＨ等から抽出された鍵書換情報Ｋを用いて、暗号化に使用された暗号鍵へと暗号鍵を書き換えた後に、書き換えた暗号鍵を用いて同期パケットを復号する（Ｓ２６）。そして、復号した同期パケットを信号処理部１１へと供給する（Ｓ２７）。

【００１５】

一方、通信パケットが非同期パケットであると判断されると（Ｓ２２）、非同期パケットP_{N2}をＤＴＣＰ部１２に供給し、ブロック暗号により復号する（Ｓ２

３）。暗号処理が時変鍵を用いられたものであれば、鍵管理部１３により、ヘッダＨの後に付加された鍵書換情報Ｋを用いて、暗号化に使用された暗号鍵へと暗号鍵を書き換えた後に、書き換えた暗号鍵を用いて非同期パケットP_{N2}を復号する。

【００１６】

その後、復号した非同期パケットP_{N2}を非同期処理部／抽出部１５に供給し、ヘッダＨの後に付加されたデータ長情報Ｌに基づいて、図２に示すように、付加データＤを除いた実データＪへと抽出する（Ｓ２４）。その後、抽出した実データＪを信号処理部１１へと供給する（Ｓ２５）。

【００１７】

こうすることにより、本発明に係る通信装置によれば、非同期パケットの情報も同期パケットと同様に、ブロック暗号等の復号を施してセキュリティを確保しつつ通信処理を行うことが可能となる。

又、更に、パケット情報のコピー回数を、例えば、１回又は０回に制限する、又は制限なくコピー可能等のコピー制御情報Ｃが非同期パケットP_{N2}のヘッダＨの後に付加されていれば、信号処理部１１では、このコピー制御情報Ｃに基づいて、非同期パケットP_{N2}が含むコンテンツである実データＪのコピー制御を行う。これにより、非同期パケットについても同期パケットと同様に、コンテンツの複写回数を制限することで、コンテンツの著作権を一定の範囲で保護することが同期パケットと同様の手法で可能となる。

又、更に、図４に示すように、これらのデータ長情報Ｌ、鍵書換情報Ｋ、コピー制御情報Ｃの制御情報が制御情報のための専用パケットP_{N3}として非同期パケットP_{N2}の間に挿入されて送信されることも可能である。非同期処理部／抽出部１５では、このような専用パケットP_{N3}から各制御情報を取り出し、以降の制御に使用するものである。これにより、同様に、非同期パケットも同期パケットと同様の手法により、時変鍵を用いた暗号化・復号処理及びコピー処理の制御を行うことが可能となる。

以上記載した様々な実施形態により、当業者は本発明を実現することができるが、更にこれらの実施形態の様々な変形例を思いつくことが当業者によって容易

であり、発明的な能力をもたなくとも様々な実施形態へと適用することが可能である。従って、本発明は、開示された原理と新規な特徴に矛盾しない広範な範囲に及ぶものであり、上述した実施形態に限定されるものではない。

【００１８】

【発明の効果】

以上詳述したように本発明によれば、暗号化のブロック長の整数倍ではない非同期パケットも、パディング処理によりデータ長を調整することで、同期パケットと同様の手法により暗号化し復号することができ、これにより、非同期パケットも同期パケットと同様にセキュリティを確保しながら通信処理を行うことができる通信装置を提供することが可能となる。

【図面の簡単な説明】

【図１】

本発明に係る通信装置であるテレビジョンの構成の一例を示すブロック図。

【図２】

本発明に係る通信装置により非同期パケットに施されるパディング処理を説明する図。

【図３】

本発明に係る通信装置によりパディング処理された非同期パケットに制御情報を付加することを説明する図。

【図４】

本発明に係る通信装置によりパディング処理された非同期パケットに制御情報の専用非同期パケットを付加することを説明する図。

【図５】

本発明に係る通信装置により非同期パケットをパディング処理して送信処理する動作を説明するフローチャート。

【図６】

本発明に係る通信装置によりパディング処理された非同期パケットを受信処理する動作を説明するフローチャート。

【図７】

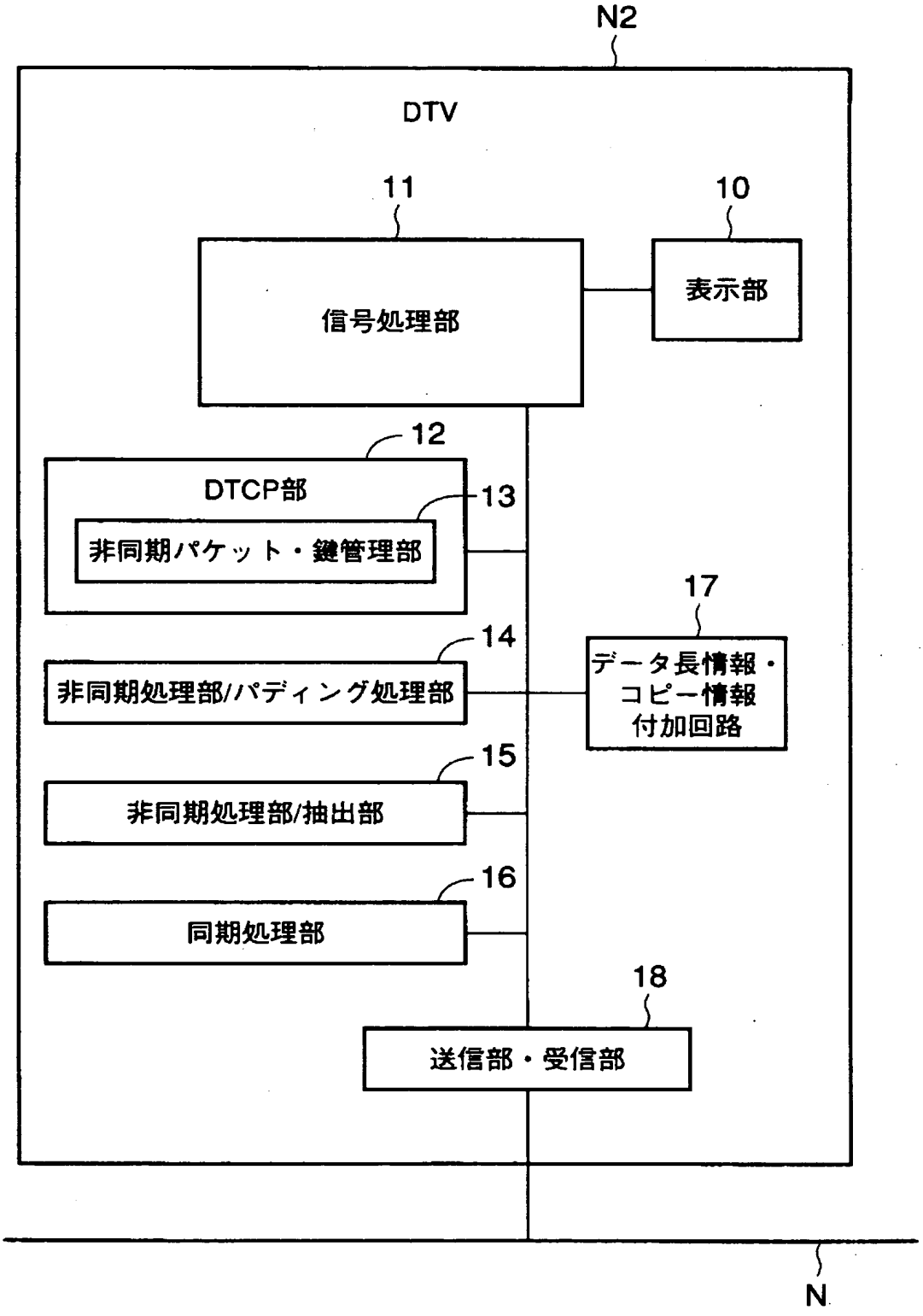
本発明に係る通信装置により構成されたネットワークシステムの一例を示すシステム図。

【符号の説明】

Ｎ２…通信装置（ＤＴＶ）、１０…表示部、１１…信号処理部、１２…ＤＴＣＰ部、１３…非同期パケット・鍵管理部、１４…非同期処理部／パディング処理部、１５…非同期処理部／抽出部、１６…同期処理部、１７…データ長情報・コピー情報付加回路、１８…送信部・受信部。

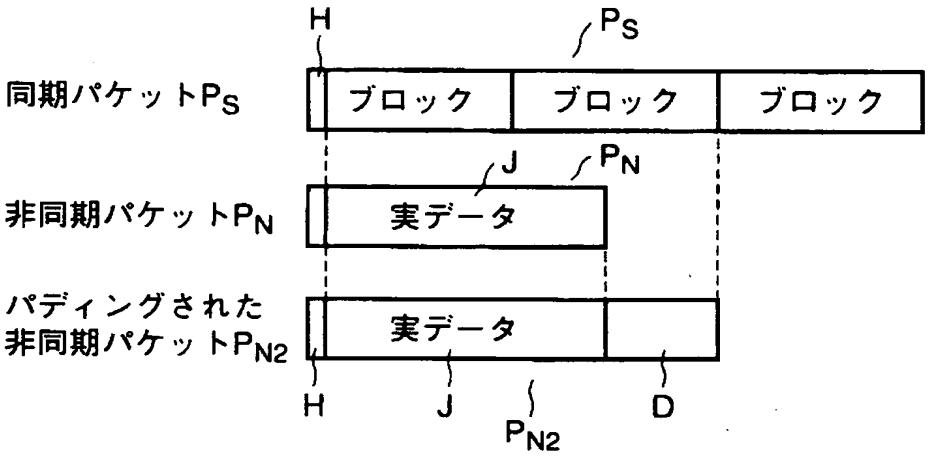
【書類名】　　図面

【図１】

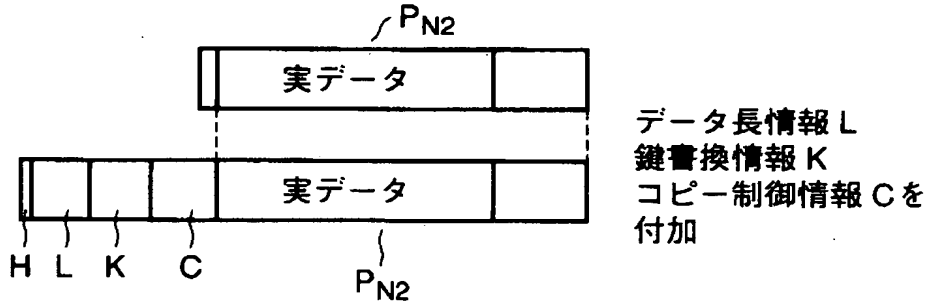


出証特２００３－３００２８１４

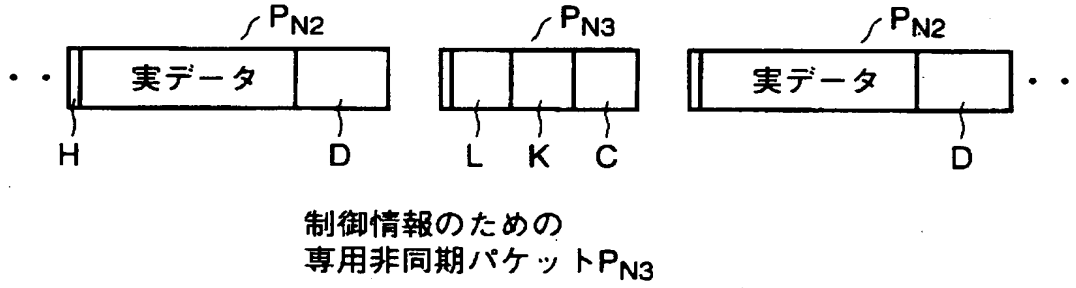
【図２】


H
PS
同期パケットPS
ブロック
ブロック
ブロック
J
PN
非同期パケットPN
実データ
パディングされた
非同期パケットPN2
実データ
H
J
D
PN2

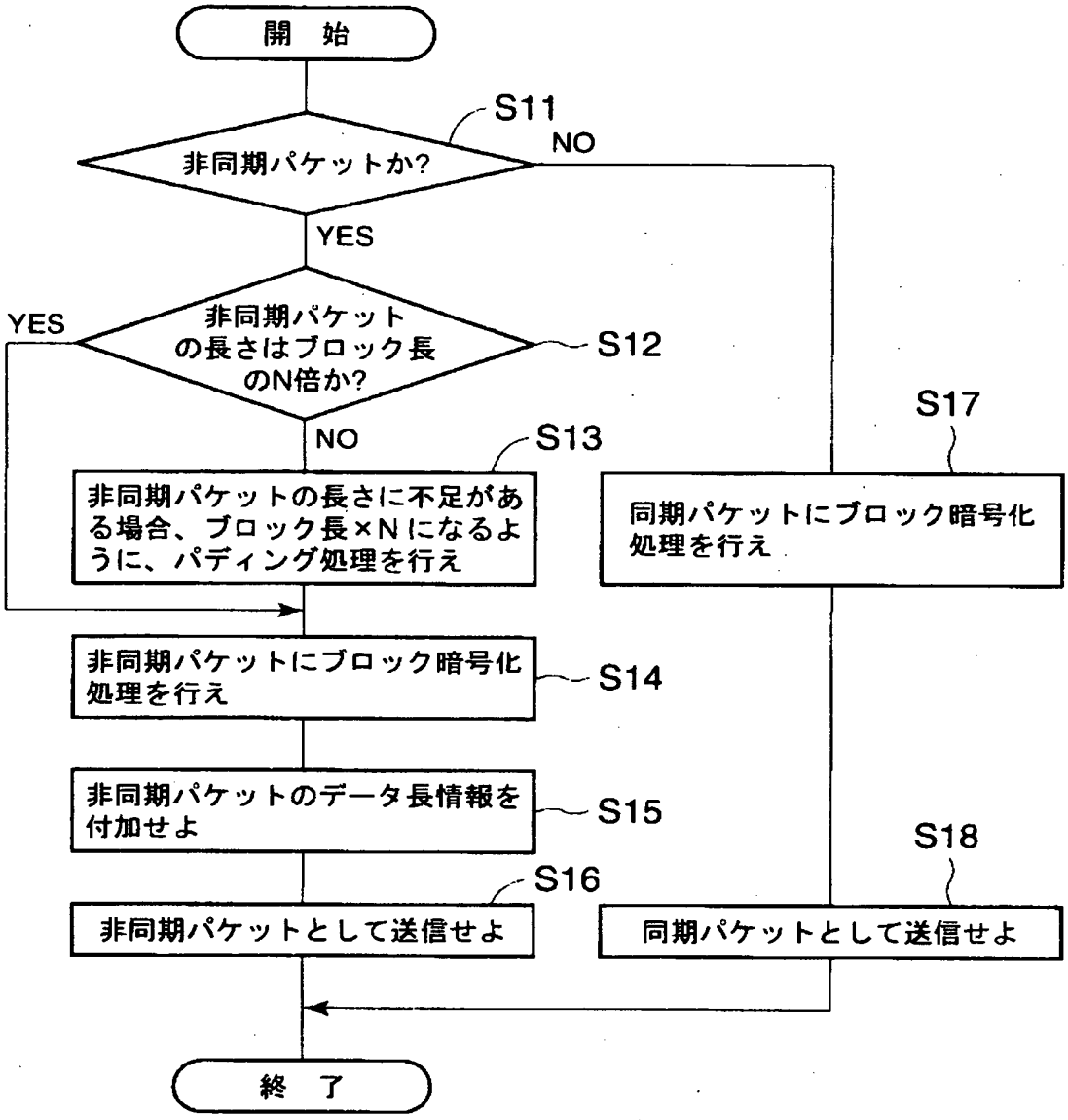
【図３】


PN2
実データ
実データ
H
L
K
C
PN2
データ長情報Ｌ
鍵書換情報Ｋ
コピー制御情報Ｃを
付加

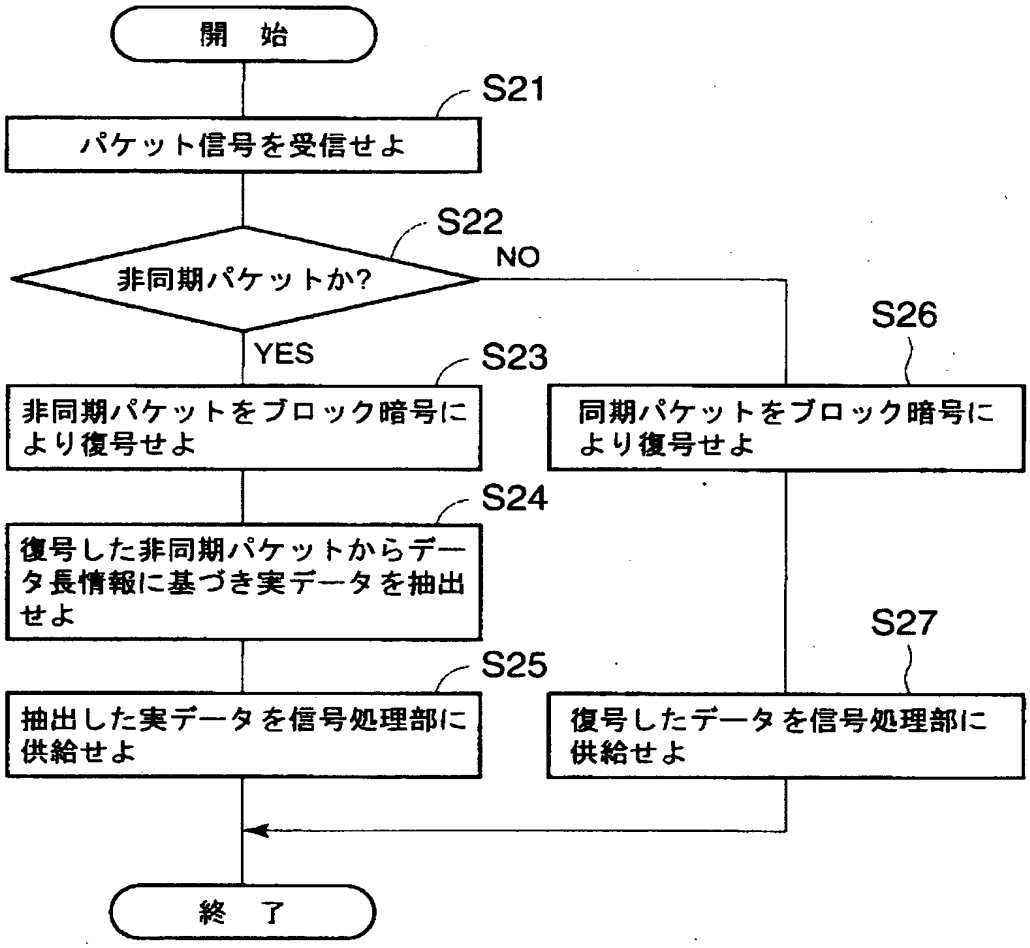
【図４】


PN2
PN3
PN2
実データ
実データ
H
D
L
K
C
D
制御情報のための
専用非同期パケットPN3

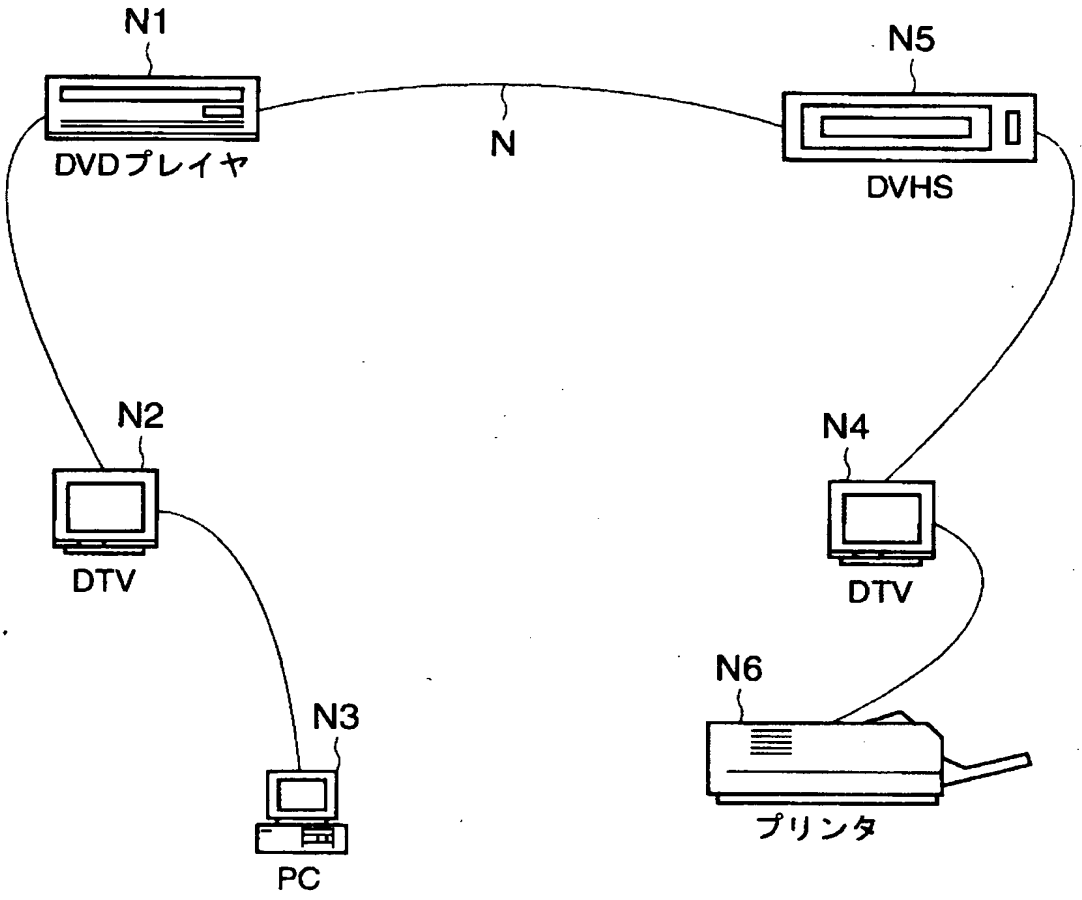
【図５】


開　始
S11
非同期パケットか?
NO
YES
非同期パケット
の長さはブロック長
のN倍か?
YES
S12
NO
S13
非同期パケットの長さに不足がある場合、ブロック長×Nになるように、パディング処理を行え
非同期パケットにブロック暗号化処理を行え
S14
非同期パケットのデータ長情報を付加せよ
S15
S16
非同期パケットとして送信せよ
S17
同期パケットにブロック暗号化処理を行え
S18
同期パケットとして送信せよ
終　了

【図６】


開　始
S21
パケット信号を受信せよ
S22
非同期パケットか?
NO
YES
S23
非同期パケットをブロック暗号により復号せよ
S24
復号した非同期パケットからデータ長情報に基づき実データを抽出せよ
S25
抽出した実データを信号処理部に供給せよ
S26
同期パケットをブロック暗号により復号せよ
S27
復号したデータを信号処理部に供給せよ
終　了

【図７】



【書類名】　　要約書

【要約】

【課題】　非同期パケットも同期パケットと同様に暗号化して通信を行う通信装置及び通信方法を提供する。

【解決手段】　非同期パケットを暗号化のブロック長の整数倍の長さにするべくデータを付加するパディング処理を施すパディング処理部と、パディング処理部によりパディング処理されたパディング非同期パケット及び同期パケットを暗号化する暗号部と、暗号化された暗号化パディング非同期パケット及び暗号化同期パケットを送信する送信部とを有する通信装置。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝